Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Daniel
Last Name: Ribakoff
Mailing Address: 6524 Genstar Ln.
City: Dallas
Country: United States
State or Province: TX
ZIP/Postal Code: 75252-5406
Email Address:
Organization Name:
Comment: It is wrong to try to control devices people own if they are not using them for illegal activities. People have the right to modify their possessions, and this cannot be taken away from us.

We rely on security researchers who investigate devices to further secure our electronics.

If the manufacturer stops supporting their product, people should be able to modify the software themselves to maintain it, otherwise, security holes will never be patched.

In the past, users have fixed serious bugs on hardware that the manufacturer has deemed "outdated." An example of this is the Linksys WRT54G, which continues to recieve comminuty support through projects such as OpenWRT and Tomato. Linksys have since commended the efforts of the community and have released another "WRT" router specifically to be modified by the community.

If the government chooses to limit what the consumers of a product can do with what they have purchased, the people of that government will live in tyranny, and for a country that proclaims itself as "free," that is unacceptable.

Do not let this pass.

It is wrong to try to control devices people own if they are not using them for illegal activities. People have the right to modify their possessions, and this cannot be taken away from us.

We rely on security researchers who investigate devices to further secure our electronics.

If the manufacturer stops supporting their product, people should be able to modify the software themselves to maintain it, otherwise, security holes will never be patched.

In the past, users have fixed serious bugs on hardware that the manufacturer has deemed "outdated." An example of this is the Linksys WRT54G, which continues to recieve comminuty support through projects such as OpenWRT and Tomato. Linksys have since commended the efforts of the community and have released another "WRT" router specifically to be modified by the community.

If the government chooses to limit what the consumers of a product can do with what they have purchased, the people of that government will live in tyranny, and for a country that proclaims itself as "free," that is unacceptable.

Do not let this pass.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: James
Last Name: Sherwood
Mailing Address: 2764 hacker rd
City: brighton
Country: United States
State or Province: MI
ZIP/Postal Code: 48114
Email Address: iamthekingofminecraft@gmail.com
Organization Name:
Comment: This is not something any normal person wants.

This is not something any normal person wants.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jared
Last Name: Sherwood
Mailing Address: 2764 hacker rd
City: brighton
Country: United States
State or Province: MI
ZIP/Postal Code: 48114
Email Address: iamthekingofminecraft@gmail.com
Organization Name: /tech/
Comment: I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.
Some points:
Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
Users should be able to manipulate and control all aspects of their devices
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
So I finally must say in my own personal opinion that this is awful in most every way and you should move to have whoever suggested it removed. If this came from a group of or singular company it wouldn't be hard to prove and cause them major damage.

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.
Some points:
Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.
Users should be able to manipulate and control all aspects of their devices
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.
So I finally must say in my own personal opinion that this is awful in most every way and you should move to have whoever suggested it removed. If this came from a group of or singular company it wouldn't be hard to prove and cause them major damage.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jesse
Last Name: Sena
Mailing Address: 9820 N. 167th E. Ave.
City: Owasso
Country: United States
State or Province: OK
ZIP/Postal Code: 74055
Email Address: jdsenaok@gmail.com
Organization Name:
Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jason
Last Name: Winzenried
Mailing Address: 1608 11th St
City: Cody
Country: United States
State or Province: WY
ZIP/Postal Code: 82414-4210
Email Address:
Organization Name:
Comment: Most routers are useless with their included firmware. The most well loved and stable routers are those that can be flashed with a venerable firmware like DD-WRT. Forbidding such aftermarket (yet old and stable) firmwares will hamper the usefulness of router hardware and stifle innovation. I am strongly against such a course of action

Most routers are useless with their included firmware. The most well loved and stable routers are those that can be flashed with a venerable firmware like DD-WRT. Forbidding such aftermarket (yet old and stable) firmwares will hamper the usefulness of router hardware and stifle innovation. I am strongly against such a course of action

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Mellissa
Last Name: Dalby
Mailing Address: 2101 Northland RD
City: Woodlawn
Country: United States
State or Province: MD
ZIP/Postal Code: 21207
Email Address: Mellissa.Dalby@gmail.com
Organization Name:
Comment: Please do not make it illegal to load LINUX and other open source software on personal computers and laptops. It is necessary to do that in order to do my job and I don't want to become an outlaw in order to keep doing my job.

Please do not make it illegal to load LINUX and other open source software on personal computers and laptops. It is necessary to do that in order to do my job and I don't want to become an outlaw in order to keep doing my job.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Sam
Last Name: LaManna
Mailing Address: 215 north 11th street
City: Reading
Country: United States
State or Province: PA
ZIP/Postal Code: 19540
Email Address:
Organization Name:
Comment: I do not at all agree with this measure

I do not at all agree with this measure

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Josh
Last Name: Katz
Mailing Address: 37 South Broadway
City: Fair Lawn
Country: United States
State or Province: NJ
ZIP/Postal Code: 07410
Email Address: gravypod@gravypod.com
Organization Name:
Comment: As a HAM this infuriates me that you would even consider something this debilitating. SDR would in essence be ruined.

As a HAM this infuriates me that you would even consider something this debilitating. SDR would in essence be ruined.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Brian
Last Name: Mangerson
Mailing Address: 4604 Poppy Court
City: Hampton
Country: United States
State or Province: VA
ZIP/Postal Code: 23666
Email Address: brian.mangerson@hotmail.com
Organization Name:
Comment: Please do not force restriction of altering, jail-breaking, or installing different firmware on wireless devices. Such a rule would be a nuclear option to solve a problem that does not really exist at scales to be relevant.

An analogy would be banning roads because bank robbers use them, or banning fixing of cars because they are used to commit crimes or look different than than manufacturer would like.

This rule would strip ownership rights of citizens that purchase devices. it means they don't really own the devices they purchase, but can only use them as someone else intends. It will make us less secure by preventing security research and will stop vital research into wireless networking technologies such as mesh networking and hamper ad-hoc emergency communications.

it would outlaw installing a different operating system on my laptop and effectively create criminals out of everyone that uses any free, open source operating systems like Linux,UNIX, or freebsd, which would in turn affect all other branches of cyber security and digital privacy research.

please don't outlaw user choice,research or privacy.

respectfully,

a concerned citizen and computer science professional.

Please do not force restriction of altering, jail-breaking, or installing different firmware on wireless devices. Such a rule would be a nuclear option to solve a problem that does not really exist at scales to be relevant.

An analogy would be banning roads because bank robbers use them, or banning fixing of cars because they are used to commit crimes or look different than than manufacturer would like.

This rule would strip ownership rights of citizens that purchase devices. it means they don't really own the devices they purchase, but can only use them as someone else intends. It will make us less secure by preventing security research and will stop vital research into wireless networking technologies such as mesh networking and hamper ad-hoc emergency communications.

it would outlaw installing a different operating system on my laptop and effectively create criminals out of everyone that uses any free, open source operating systems like Linux,UNIX, or freebsd, which would in turn affect all other

branches of cyber security and digital privacy research.

please don't outlaw user choice,research or privacy.

respectfully,

a concerned citizen and computer science professional.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Ethan
Last Name: Tom
Mailing Address: 151 Idlewood Dr.
City: Stamford
Country: United States
State or Province: CT
ZIP/Postal Code: 06905
Email Address:
Organization Name:
Comment: I am asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This is very clearly a bad idea, for several reasons.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

I respectfully ask the FCC to discard this idea, and to focus on making the web, a crucial source of information, more open and free. This not only benefits the people, but the country and society as a whole.

I am asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. This is very clearly a bad idea, for several reasons.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Mesh networking which helps first responders in emergencies, also helps provide anonymity, creates a backup/alternative communications network, will become more difficult than it needs to be with these new rules.

Users should be able to manipulate and control all aspects of their devices.
The ability to run fully open source software on your devices will be severely hampered and possibly impossible with these new rules.

I respectfully ask the FCC to discard this idea, and to focus on making the web, a crucial source of information, more open and free. This not only benefits the people, but the country and society as a whole.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Anthony
Last Name: Tarpley
Mailing Address: 11934 canyon valley dr
City: Tomba
Country: United States
State or Province: TX
ZIP/Postal Code: 77377
Email Address: Homelesscarl@hotmail.com
Organization Name: None
Comment:

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Tom
Last Name: Corbin
Mailing Address: 5602 Narsonne Street
City: Corpus Christi
Country: United States
State or Province: TX
ZIP/Postal Code: 78414
Email Address: tom.corbin@gmail.com
Organization Name:
Comment: I am against this proposed regulation. Router manufacturers seldom if at all update firmware on their routers thereby leaving them open to malicious exploits. I regularly update the firmware on my Asus router using Asuswrt-Merlin open source software. This allows my router to be secure from malicious attacks.

I am against this proposed regulation. Router manufacturers seldom if at all update firmware on their routers thereby leaving them open to malicious exploits. I regularly update the firmware on my Asus router using Asuswrt-Merlin open source software. This allows my router to be secure from malicious attacks.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: David
Last Name: Fink
Mailing Address: 588 35th street
City: Ogden
Country: United States
State or Province: UT
ZIP/Postal Code: 84403
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Solomon
Last Name: Alpert
Mailing Address: 2490 Channing Way, Apt. 213A
City: Berkeley
Country: United States
State or Province: CA
ZIP/Postal Code: 94704
Email Address: soli.r.alpert@gmail.com
Organization Name:
Comment: People should be able to put whatever software on whatever technology they legally own. Period.The FCC should not restrict which OS you choose to use on your personally owned, lawfully obtained computer.

People should be able to put whatever software on whatever technology they legally own. Period.The FCC should not restrict which OS you choose to use on your personally owned, lawfully obtained computer.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Sean
Last Name: Falconer
Mailing Address: 1238 S. Rosewood Ave.
City: Santa Ana
Country: United States
State or Province: CA
ZIP/Postal Code: 92707
Email Address: seanfalconer@yahoo.com
Organization Name:
Comment: Please do NOT do this and remove any mention of not allowing third party firm waste on network devices. I use dd-wrt exclusively to allow me to setup test Labs that mimic my larger enterprise networks. In addition it allows me to do many things that would be too costly for the average home enthusiast otherwise.   Not to mention the significant number of coffee contributors, testers, etc in the technology field who make this software possible. REMOVE ANY CLAUSES THAT DISALLOW THE USE OF THIS PARTY FIRMWARE.

Please do NOT do this and remove any mention of not allowing third party firm waste on network devices. I use dd-wrt exclusively to allow me to setup test Labs that mimic my larger enterprise networks. In addition it allows me to do many things that would be too costly for the average home enthusiast otherwise.   Not to mention the significant number of coffee contributors, testers, etc in the technology field who make this software possible. REMOVE ANY CLAUSES THAT DISALLOW THE USE OF THIS PARTY FIRMWARE.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Quang
Last Name: Vu
Mailing Address: 37 Berks Ct
City: Quakertown
Country: United States
State or Province: PA
ZIP/Postal Code: 18951
Email Address: shuttle099@outlook.com
Organization Name:
Comment: The FCC should consider not implementing the proposal to take away the ability to install software other than the manufacture. This may render Linux and other OS's from being installed on manufactured PC, and force users to only use manufactured softwares which may lack customization or lack security fixes.

The FCC should consider not implementing the proposal to take away the ability to install software other than the manufacture. This may render Linux and other OS's from being installed on manufactured PC, and force users to only use manufactured softwares which may lack customization or lack security fixes.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Randal
Last Name: Torris
Mailing Address: 15859 NE Davis St
City: Portland
Country: United States
State or Province: OR
ZIP/Postal Code: 97230
Email Address: rtorris@gmail.com
Organization Name:
Comment: I understand the need to control some aspects of hardware such as power transmission.

I feel that stopping all firmware changes to be too much.
I have made use of DDWRT, OpenWRT to turn old and thrown out equipment into useful and productive items.

Please find another way to control what should be controlled.

I understand the need to control some aspects of hardware such as power transmission.

I feel that stopping all firmware changes to be too much.
I have made use of DDWRT, OpenWRT to turn old and thrown out equipment into useful and productive items.

Please find another way to control what should be controlled.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Michael
Last Name: Donnelly
Mailing Address: POB 544
City: Lincoln
Country: United States
State or Province: AL
ZIP/Postal Code: 35096
Email Address: IamEqualtoall@gmail.com
Organization Name: null
Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Leonardo
Last Name: Taborda ngel
Mailing Address: Calle 32 sur # 51a56
City: Bogot
Country: Colombia
State or Province: Cundinamarca
ZIP/Postal Code: 111621272
Email Address: leonardotaborda@networkbogota.org
Organization Name: Network Bogot
Comment: Who may it concern

I am really worried about the FCC proposal, where you want to force WiFi device vendors and manufacters to create and deploy measures in order to prevent end-users to modify and install third party firmware for example on home routers and others.

That idea itself it's threat for many civil rights not only in the U.S but worldwide. We, the users, have the right and the will to modify any given wifi device in order to make it capable of other functions the vendor didn't envisioned it when created such device, extend the lifetime of a device that may cost a lot in countries outside the US, by modifying its firmware thus, saving money, avoiding electronic waste and so on.

That proposal is a terrible news for a really big important movement nowadays, the movement of free, open and decentralized wireless networks. Many of them rely on modified firmware devices in order to work. These networks have already provided internet to rural areas, serve as a backup when there's no internet by providing local contents, aim the creation and sharing of free and local content, the open and costless comunication and even could help in disaster situations.

Please, reconsider the way yo want to run the proposal on preventing third-party firmware modificiations. It is a big threat to many positive and kind initiatives around the world that rely on the capability to modify wifi devices.

Who may it concern

I am really worried about the FCC proposal, where you want to force WiFi device vendors and manufacters to create and deploy measures in order to prevent end-users to modify and install third party firmware for example on home routers and others.

That idea itself it's threat for many civil rights not only in the U.S but worldwide. We, the users, have the right and the will to modify any given wifi device in order to make it capable of other functions the vendor didn't envisioned it when created such device, extend the lifetime of a device that may cost a lot in countries outside the US, by modifying its firmware thus, saving money, avoiding electronic waste and so on.

That proposal is a terrible news for a really big important movement nowadays, the movement of free, open and decentralized wireless networks. Many of them rely on modified firmware devices in order to work. These networks have already provided internet to rural areas, serve as a backup when there's no internet by providing local contents, aim

the creation and sharing of free and local content, the open and costless comunication and even could help in disaster situations.

Please, reconsider the way yo want to run the proposal on preventing third-party firmware modificiations. It is a big threat to many positive and kind initiatives around the world that rely on the capability to modify wifi devices.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Mitesh
Last Name: Patel
Mailing Address: 210 Coleman Blvd Apt T1
City: Charleston
Country: United States
State or Province: SC
ZIP/Postal Code: 29464
Email Address: mitesh324@gmail.com
Organization Name: SPAWAR
Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

These comments were not written by me, however I agree with the statements they are saying. If I'm unable to have control over my own device, then I do not truly own what I bought. To me this is also a case of ownership of a physical device, which I paid for my own personal use.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

These comments were not written by me, however I agree with the statements they are saying. If I'm unable to have control over my own device, then I do not truly own what I bought. To me this is also a case of ownership of a physical device, which I paid for my own personal use.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Zev
Last Name: Chonoles
Mailing Address: 105 Spring Road
City: Malvern
Country: United States
State or Province: PA
ZIP/Postal Code: 19355-2112
Email Address:
Organization Name:
Comment: Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely

bad" category of regulatory ideas.

Public servants of the Federal Communications Commission,

It is with great concern that I write you today regarding the latest proposal to restrict free use and research by private citizens of alternative wireless and computing systems.

The ability for private citizens alongside, but not in conjunction with, federally approved researchers to conduct their own research and use of any and all methods of electronic communication is paramount to the future progress of technological advancement of this very necessary field of technology.

On the subject of liberty it is not at all acceptable that, given we live in a free society, our use of technology should be dependent upon federal approval of certain manufacturer's technology nor should our separate but intersecting third party devices be limited by some arbitrarily concocted regulations. It is not within the federal government's powers or mandate to codify specific software and hardware solely on the basis that it lies outside standard mainstream consumer products. Further, information security is paramount in today's world and often alternative operating systems offer a higher degree of internal systems security not found in most popular and conventional forms of consumer products. The FCC could find itself in quite a precarious position should a large number of citizens find their data in the hands of unscrupulous individuals which could have been averted were they able to use alternative technology systems but were denied due to the FCC's own regulatory measures.

Americans must also be able to secure their own data when the companies we rely on abstain from patching their own security flaws. That the FCC would be considering a proposal which could leave private citizens at the mercy of individuals operating outside the boundaries of the law is worrisome to say the least and in the past it has often been the case that privacy gaps and security flaws in wireless hardware which transmits sensitive data has been fixed as a result of the efforts of private individuals. This and many similar actions would be banned under the NPRM.

The FCC may also run afoul of the First Amendment to the Constitution by limiting those citizens who seek to use alternative methods and hardware to transmit wireless data as a matter of political principals and the desire to express political dissent through legitimate consumption practices. The NPRM would stifle this very legitimate speech, protected under the First Amendment, and may find itself on the wrong side of Constitutional Law and Supreme Court precedent.

I hope my words have not been met by deaf ears and the Federal Communications Commission takes seriously the implications of this very dangerous precedent being set should this regulatory measure come into effect. I am confident in the FCC's ability to make the right choice by setting aside this regulatory measure and hanging it up in the "extremely bad" category of regulatory ideas.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Josh
Last Name: Peters
Mailing Address: Rm 1108, Margret Loock Hall, 324 E. Juneau Ave.
City: Milwaukee, WI
Country: United States
State or Province: WI
ZIP/Postal Code: 53202
Email Address: petersjt@msoe.edu
Organization Name: Milwaukee School of Engineering
Comment: This is an affront to both privacy and innovation.

If any person wishes to modify their router for increased security, extra features, or increased range, they should be free to do so. Not only would this proposal kill projects like DD-WRT and OpenWRT, it would compromise the security of routers in general.

Any plan that requires locking down hardware in this manner prevents the end user from being completely secure; Without having full control of their device, a user cannot be certain they are not being monitored. After the spying activities of the NSA and GHCQ were revealed, this cannot be more relevant.

Please, In the name American security and peace of mind, I urge you to dismiss this proposal. Thank you for your time.

This is an affront to both privacy and innovation.

If any person wishes to modify their router for increased security, extra features, or increased range, they should be free to do so. Not only would this proposal kill projects like DD-WRT and OpenWRT, it would compromise the security of routers in general.

Any plan that requires locking down hardware in this manner prevents the end user from being completely secure; Without having full control of their device, a user cannot be certain they are not being monitored. After the spying activities of the NSA and GHCQ were revealed, this cannot be more relevant.

Please, In the name American security and peace of mind, I urge you to dismiss this proposal. Thank you for your time.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Eric
Last Name: Lamberson
Mailing Address: 22118 Cristobal Dr
City: Garden Ridge
Country: United States
State or Province: TX
ZIP/Postal Code: 78266
Email Address: ericlamberson@gmail.com
Organization Name: American Citizen
Comment: I am absolutely against any rule that prevents legitimate owners of RF devices from changing or upgrading device firmware. This rule change is unnecessary.

I am absolutely against any rule that prevents legitimate owners of RF devices from changing or upgrading device firmware. This rule change is unnecessary.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Donald
Last Name: Campbell
Mailing Address: 7711 Granny Valley Rd
City: Gloucester
Country: United States
State or Province: VA
ZIP/Postal Code: 23061
Email Address: donald.campbell@wildblue.net
Organization Name:
Comment: In this proposal, the FCC mandates that manufacturers be institutionally protected and allowed to rape the American Consumer.

It has been repeatedly demonstrated, at sites such as: dd-wrt dot com that manufacturers typically provide minimally enabled software, often restricting usages that the hardware is easily capable of performing. The manufacturer, naturally, has an additional router product with the capability, at a higher price, often with almost identical hardware.

One need look no farther than IOS and Android for examples of software that manufacturer's can 'lock' the owner of the device from deleting software placed there for the manufacturer's convenience, not the owner. The capability to have 'root access' is denied to the device's owner... A feat Microsoft hasn't even tried to accomplish, although 'Trusted Installer' is a step in that (wrong) direction.

For a fast and dynamic software/hardware industry, the Federal Government's over regulation and bureaucratic need for control protect existing manufacturers and provide an unnecessary barrier to new, better and cheaper products from entering the market.

In this proposal, the FCC mandates that manufacturers be institutionally protected and allowed to rape the American Consumer.

It has been repeatedly demonstrated, at sites such as: dd-wrt dot com that manufacturers typically provide minimally enabled software, often restricting usages that the hardware is easily capable of performing. The manufacturer, naturally, has an additional router product with the capability, at a higher price, often with almost identical hardware.

One need look no farther than IOS and Android for examples of software that manufacturer's can 'lock' the owner of the device from deleting software placed there for the manufacturer's convenience, not the owner. The capability to have 'root access' is denied to the device's owner... A feat Microsoft hasn't even tried to accomplish, although 'Trusted Installer' is a step in that (wrong) direction.

For a fast and dynamic software/hardware industry, the Federal Government's over regulation and bureaucratic need for control protect existing manufacturers and provide an unnecessary barrier to new, better and cheaper products from entering the market.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Soren
Last Name: Stoutner
Mailing Address: 635 North Heights Road
City: Wickenburg
Country: United States
State or Province: AZ
ZIP/Postal Code: 85390
Email Address: soren@smallbusinesstech.net
Organization Name: Small Business Tech Solutions
Comment: Innovation
Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact
Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Guest Wifi hotspots businesses
Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses
Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: John
Last Name: Windsor
Mailing Address: 291 NW 46 Street
City: Pompano Beach
Country: United States
State or Province: FL
ZIP/Postal Code: 33064
Email Address: scott63@gmail.com
Organization Name: null
Comment: I would like to request that you do not implement any new rules or regulations that prohibit or inhibit Americans from installing software or modifying electronic devices or computers that they own.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I would like to request that you do not implement any new rules or regulations that prohibit or inhibit Americans from installing software or modifying electronic devices or computers that they own.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Allen
Last Name: Tipper
Mailing Address: 3119 Ronald St
City: Lansing
Country: United States
State or Province: MI
ZIP/Postal Code: 48911-2641
Email Address: akerasi@gmail.com
Organization Name:
Comment: This rule would be yet another rule removing power from consumers and handing it off to large corporations. I bet you think that's a good thing. I don't.

This rule would be yet another rule removing power from consumers and handing it off to large corporations. I bet you think that's a good thing. I don't.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Karl
Last Name: Berry
Mailing Address: 88609 Wickizer Ln
City: Bandon
Country: United States
State or Province: OR
ZIP/Postal Code: 97411
Email Address:
Organization Name:
Comment: Please do not create rules forbidding people to install software of their own choice on their own computing devices, of any sort. Thanks.

Please do not create rules forbidding people to install software of their own choice on their own computing devices, of any sort. Thanks.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Richard
Last Name: Brown
Mailing Address: 84 Orford Road
City: Lyme
Country: United States
State or Province: NH
ZIP/Postal Code: 03768
Email Address: richb.hanover@gmail.com
Organization Name: Blueberry Hill Software
Comment: I would formally request a 30-day extension to this comment period.

The original deadline was very short - only a week or so from the end of the NPRM cutoff to the 8 Sep 2015 deadline for comments.

There is tremendous interest in this subject from the various communities who are expected to be affected by this Proposed Rule, and it would only be fair to allow them to make their comments heard.

I would formally request a 30-day extension to this comment period.

The original deadline was very short - only a week or so from the end of the NPRM cutoff to the 8 Sep 2015 deadline for comments.

There is tremendous interest in this subject from the various communities who are expected to be affected by this Proposed Rule, and it would only be fair to allow them to make their comments heard.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Christopher
Last Name: Welles
Mailing Address: 1 Shore Ln Apt 2507
City: Jersey City
Country: United States
State or Province: NJ
ZIP/Postal Code: 07310
Email Address: cwelles@quantix.com
Organization Name:
Comment: I have relied on various open source firmware packages for my routers for over a decade. I have done this, not for fun or curiosity, but because it has been the only option available that provides the functionality necessary to make everything on my network work properly. In addition, it provides far more detail as far as logging and traffic analysis go, thus providing the only reasonable option for me as far as security is concerned.

Generally vendor WiFi firmware has been significantly ahead of open source for wireless functionality. Because of this, I have tried a two device setup before, where the router is open source, and the wireless access point uses vendor firmware. This, unfortunately has functional limitations and I've been forced to go back a single device with open source firmware.

Despite what some may think, small office / home networking is a very immature technology. Perhaps Google, Apple, or Microsoft will finally crack it and make it all invisible. Until then, open source firmware is vital for enable folks to "get things done". I use Windows desktops, apple mobile devices, and a hell of a lot of google services. I'm not an open source fanatic of any sort, but it's use in wireless routes has been critical for me.

I have relied on various open source firmware packages for my routers for over a decade. I have done this, not for fun or curiosity, but because it has been the only option available that provides the functionality necessary to make everything on my network work properly. In addition, it provides far more detail as far as logging and traffic analysis go, thus providing the only reasonable option for me as far as security is concerned.

Generally vendor WiFi firmware has been significantly ahead of open source for wireless functionality. Because of this, I have tried a two device setup before, where the router is open source, and the wireless access point uses vendor firmware. This, unfortunately has functional limitations and I've been forced to go back a single device with open source firmware.

Despite what some may think, small office / home networking is a very immature technology. Perhaps Google, Apple, or Microsoft will finally crack it and make it all invisible. Until then, open source firmware is vital for enable folks to "get things done". I use Windows desktops, apple mobile devices, and a hell of a lot of google services. I'm not an open source fanatic of any sort, but it's use in wireless routes has been critical for me.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: jan
Last Name: paulus
Mailing Address: jan.paulus@hotmail.com
City: bruxelles
Country: Belgium
State or Province: BRUXELLES
ZIP/Postal Code: 1001
Email Address: jan.paulus@hotmail.com
Organization Name:
Comment: Hi,

like usual I will continue to use and to buy material I can manage, upgrade and protect as I want. The rest I never buy it.

Think it's time to start for other people to do the same and to stop buy material from those companies that will propose them.

Hi,

like usual I will continue to use and to buy material I can manage, upgrade and protect as I want. The rest I never buy it.

Think it's time to start for other people to do the same and to stop buy material from those companies that will propose them.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Fabien
Last Name: Marsaud
Mailing Address: 44 rue Ferbeyre
City: Bordeaux
Country: France
State or Province: Aquitaine
ZIP/Postal Code: 33200
Email Address: fabmars@gmail.com
Organization Name:
Comment: HAving wireless devices locked down would be counter productive, since it would become impossible to plug newly discovered security holes. Security and the protection of personal information is an increasinly hot topic, so it's utterly important to enable every citizen to protect himself and other security-aware organizations to help them do so.

Besides such a measure looks like another attempt to enforce planned obsolescence.

HAving wireless devices locked down would be counter productive, since it would become impossible to plug newly discovered security holes. Security and the protection of personal information is an increasinly hot topic, so it's utterly important to enable every citizen to protect himself and other security-aware organizations to help them do so.

Besides such a measure looks like another attempt to enforce planned obsolescence.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Timothy
Last Name: Dougherty
Mailing Address: 80 Parkway Blvd
City: Ronkonkoma
Country: United States
State or Province: NY
ZIP/Postal Code: 11779
Email Address: tim@thebrewerscollective.com
Organization Name: The Brewers Collective
Comment: I write to urge you to discard this legislation in the name of freedom and the advancement of our species through technology.

Wireless networking is an integral part of our current and future use of interconnected systems and to be able to research and develop this further, people need the ability to modify their devices at will. Limiting the ability for businesses or individuals to modify the technology that they own has great potential to limit advancements and ideas and could open up avenues for unsavory business practices from specific vendors.

Removing the ability to modify ones own hardware in an age where manufacturers are sometimes years behind fixing issues can leave some people vulnerable for extended periods of time, and these days many people trust their personal information, financial reputations etc to be securely held on their personal devices.

Any legislation to limit the installation of 'alternative operating systems' (e.g. GNU/Linux or *BSD) is an absolute insult to the spirit of innovation and freedom. Wrapping legislation around it & limiting the spectrum of legal operating-system choices is about as ridiculous as creating laws about what colors you're allowed to like, or what music you can or cannot listen to.

I write to urge you to discard this legislation in the name of freedom and the advancement of our species through technology.

Wireless networking is an integral part of our current and future use of interconnected systems and to be able to research and develop this further, people need the ability to modify their devices at will. Limiting the ability for businesses or individuals to modify the technology that they own has great potential to limit advancements and ideas and could open up avenues for unsavory business practices from specific vendors.

Removing the ability to modify ones own hardware in an age where manufacturers are sometimes years behind fixing issues can leave some people vulnerable for extended periods of time, and these days many people trust their personal information, financial reputations etc to be securely held on their personal devices.

Any legislation to limit the installation of 'alternative operating systems' (e.g. GNU/Linux or *BSD) is an absolute insult to the spirit of innovation and freedom. Wrapping legislation around it & limiting the spectrum of legal operating-system choices is about as ridiculous as creating laws about what colors you're allowed to like, or what music you can or cannot listen to.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Steven
Last Name: Gallo
Mailing Address: 111 Harvest Dr
City: Brewster
Country: United States
State or Province: NY
ZIP/Postal Code: 10509
Email Address: null
Organization Name: null
Comment: The FCC to not implement rules that take away the ability of users to install the software/firmware of their choosing on their computing devices. Since the FCC will not implement rules to force the manufactures to fix security bugs in their products FOR THE LIFE OF THE PRODUCTS, then the FCC has no right to prevent others from doing so.
In stead, the FCC should be implementing rules that prevent Wireless Carriers from taking over the WiFi spectrum to unload their networks which is what the carriers are currently attempting to do.

The FCC to not implement rules that take away the ability of users to install the software/firmware of their choosing on their computing devices. Since the FCC will not implement rules to force the manufactures to fix security bugs in their products FOR THE LIFE OF THE PRODUCTS, then the FCC has no right to prevent others from doing so.
In stead, the FCC should be implementing rules that prevent Wireless Carriers from taking over the WiFi spectrum to unload their networks which is what the carriers are currently attempting to do.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: William
Last Name: Barratt
Mailing Address: 2024 Peach Orchard Dr Apt 24
City: Falls Church
Country: United States
State or Province: VA
ZIP/Postal Code: 22043
Email Address:
Organization Name:
Comment: The FCC should reconsider its proposed changes to the rules governing RF devices. The current proposal would have a serious detrimental effect on innovation and consumers' ability to control their own electronic devices, such as Wi-Fi routers. The risk posed by third-party software and firmware on these devices is minimal, but the benefits are immense. In many cases, the manufacturer's firmware is poorly designed and contains security holes that leaves home and corporate networks vulnerable to hacking. In other cases, manufacturer firmware prevents consumers from using or adjusting even basic network functions. As devices age, manufacturers stop releasing firmware updates for them, and leave serious security vulnerabilities unpatched.

As a result, many consumers, including me, have chosen to install third-party firmware such as OpenWRT or DD-WRT on our routers. Far from causing undesirable RF interference or other negative consequences, open-source firmware allows consumers better control over their devices, which often includes better security. It has the added benefit of saving money and reducing e-waste by breathing new life into older hardware. Third-party firmware also allows for innovation that would not be possible with the limited functionality of factory-installed firmware. Scientists and inventors would have fewer options for developing new Wi-Fi-based devices and technologies if they were not free to tinker and test with open-source firmware. Any regulation which requires FCC or manufacturer approval for third-party software or firmware will be very harmful to network security, consumer choice, and innovation in the United States and elsewhere.

The FCC should reconsider its proposed changes to the rules governing RF devices. The current proposal would have a serious detrimental effect on innovation and consumers' ability to control their own electronic devices, such as Wi-Fi routers. The risk posed by third-party software and firmware on these devices is minimal, but the benefits are immense. In many cases, the manufacturer's firmware is poorly designed and contains security holes that leaves home and corporate networks vulnerable to hacking. In other cases, manufacturer firmware prevents consumers from using or adjusting even basic network functions. As devices age, manufacturers stop releasing firmware updates for them, and leave serious security vulnerabilities unpatched.

As a result, many consumers, including me, have chosen to install third-party firmware such as OpenWRT or DD-WRT on our routers. Far from causing undesirable RF interference or other negative consequences, open-source firmware allows consumers better control over their devices, which often includes better security. It has the added benefit of saving money and reducing e-waste by breathing new life into older hardware. Third-party firmware also allows for innovation that would not be possible with the limited functionality of factory-installed firmware. Scientists and inventors would have fewer options for developing new Wi-Fi-based devices and technologies if they were not free to tinker and test with open-source firmware. Any regulation which requires FCC or manufacturer approval for third-party software or firmware will be very harmful to network security, consumer choice, and innovation in the United States

and elsewhere.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Adam
Last Name: Stohl
Mailing Address: 708 Gravenstein Hwy N #146
City: Sebastopol
Country: United States
State or Province: CA
ZIP/Postal Code: 95472
Email Address: synergysymphony@gmail.com
Organization Name:
Comment: As a IT professional, I must strongly dis-recommend this proposal.

It would be nothing short of disastrous to the security and privacy of millions of users and will only get worse over time.

Security research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Not fixing security holes either feeds cyber-threats or increases electronic waste.

As shown in the links below, the android ecosystem is a perfect example of what happens when companies stop providing security updates for older phones, leaving large portions of users insecure, As opposed to custom 3rd party firmware projects that receive frequent updates that fix vulnerabilities.

https://youtu.be/9kJsOHwAho4?t=2m2s

https://developer.android.com/about/dashboards/index.html

http://opensignal.com/reports/2015/08/android-fragmentation/

As a IT professional, I must strongly dis-recommend this proposal.

It would be nothing short of disastrous to the security and privacy of millions of users and will only get worse over time.

Security research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Not fixing security holes either feeds cyber-threats or increases electronic waste.

As shown in the links below, the android ecosystem is a perfect example of what happens when companies stop providing security updates for older phones, leaving large portions of users insecure, As opposed to custom 3rd party firmware projects that receive frequent updates that fix vulnerabilities.

https://youtu.be/9kJsOHwAho4?t=2m2s

https://developer.android.com/about/dashboards/index.html

http://opensignal.com/reports/2015/08/android-fragmentation/

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Robert
Last Name: Gorman
Mailing Address: 165 Maplewood St
City: Watertown
Country: United States
State or Province: MA
ZIP/Postal Code: 02472
Email Address: bob.gorman@gmail.com
Organization Name:
Comment: User Freedom
As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation
Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware,developed a fixfor an important form of network congestion called Bufferbloat. This fix is wasaddedto the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt andmuch research and implementation on mesh networkinghas occurred outside of manufacturers.Nearly 7,200 scholarly articleson wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact
Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5]At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Commercial VPN services businesses
Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.
Emergency Preparedness
Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is

a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware likeBroadband-Hamnetto create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers[6]designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one hadcritical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

User Freedom

As written, the rules and recommendations of the commission will prevent the installation of traditional free and open source wireless firmware such as OpenWrt. End-users often use such firmware because it better fits the users needs. Each user is better able to tailor the device to their needs. Users often set up a guest wireless network for their home or business, set up a web server at their home, create IoT hubs and other uses. The changes proposed will make such changes difficult and, in some cases, impossible.

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware,developed a fixfor an important form of network congestion called Bufferbloat. This fix is wasaddedto the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt andmuch research and implementation on mesh networkinghas occurred outside of manufacturers.Nearly 7,200 scholarly articleson wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5]At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware likeBroadband-Hamnetto create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers[6]designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one hadcritical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: cahen
Last Name: rodolphe
Mailing Address: rodolphe.cahen@gmail.com
City: grenoble
Country: France
State or Province: none applicable
ZIP/Postal Code: 38000
Email Address: rodolphe.cahen@gmail.com
Organization Name: HP France
Comment: dear sir,

I would like to pinpoint the stupidy of your proposal...

As an example, my smatphone is equipped with a wifi module, and comes with a firmware and a full pieces of software ... following your rfc, flashing the firmware or the software would be impossible ... unfortunatly, what will happen if a flaw or a security holes is found ??? if we follow your proposal, my hardware will just becomes a "nice piece od crap", unsecure and useless !!!

Wireless networking research depends on the ability of researchers to investigate and modify their devices. your proposal is simply killing this assertion.

people need the ability to fix security holes in their devices when the manufacturer chooses to not do so !!! using almteernate software like DD-WRT ...

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. NPRM will kill the innovation.

Not fixing security holes either feeds cyberthreats or increases electronic waste, and i can't imagine a world stuck in nowhere because of the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. As my company !!!! and i dont want to be led of because of the stupidity of NPRM.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. And i am pretty sure the contrary is more tru.

dear sir,

I would like to pinpoint the stupidy of your proposal...

As an example, my smatphone is equipped with a wifi module, and comes with a firmware and a full pieces of software ... following your rfc, flashing the firmware or the software would be impossible ... unfortunatly, what will happen if a flaw or a security holes is found ??? if we follow your proposal, my hardware will just becomes a "nice piece od crap", unsecure and useless !!!

Wireless networking research depends on the ability of researchers to investigate and modify their devices. your proposal is simply killing this assertion.

people need the ability to fix security holes in their devices when the manufacturer chooses to not do so !!! using almteernate software like DD-WRT ...

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. NPRM will kill the innovation.

Not fixing security holes either feeds cyberthreats or increases electronic waste, and i can't imagine a world stuck in nowhere because of the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. As my company !!!! and i dont want to be led of because of the stupidity of NPRM.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware. And i am pretty sure the contrary is more tru.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Paul
Last Name: Gardner-Stephen
Mailing Address: 10 Minchinbury Tce
City: Marion
Country: Australia
State or Province: South
ZIP/Postal Code: 5043
Email Address: paul.gardner-stephen@flinders.edu.au
Organization Name: Flinders University
Comment: Please see the attached document containing my comments.

Yours sincerely,
Dr. Paul Gardner-Stephen.

Please see the attached document containing my comments.

Yours sincerely,
Dr. Paul Gardner-Stephen.

Greetings,

I note with interest your efforts to update the rules concerning the integrity of firmware on wireless devices operating in particular bands, specifically requiring vendors to prevent the installation of 3rd-party or modified firmware on such devices.

This is of direct relevance to my humanitarian telecommunications research work at Flinders University, which is supported by the US Government through USAID.

In short, I have serious concerns about the effectiveness of the proposed rule for its intended purpose, and that any effectiveness that it might have will be greatly outweighed by collateral damage to endeavors such as mine, to other humanitarian responders, such as amateur radio operators, as well as to innovative businesses who make use of wireless router hardware, and that it will also place American businesses at a competitive disadvantage with regard to their international competitors.

I wish to make several points regarding this matter, that will hopefully explain why this proposed rule will be both ineffective and counterproductive, and should be discarded.

1. The rule will affect only equipment made for the US market. Persons will, as currently occurs, import equipment made for other markets, which will not have such protections, and indeed as is currently most likely the case, will be the greatest source of interference due to use of differing channels, bands and output power levels compared with what is allowed in the USA. Thus what is most likely the major source of interference will not be hindered at all.

2. The rapid time-to-market and low margins of most wireless devices means that software quality often suffers. In particular, firmware frequently has many vulnerabilities. Locking down firmware will prevent end users accessing 3rd-party supplied security fixes for these devices. This is particularly relevant because vendors tend to not support devices for a long period of time, and are often neither interested nor strongly engaged with providing timely security updates for older models of low-margin devices, in part because of the lack of R&D resources due to the low margins, and in part because such products compete with their newer products.

3. Related to the above point, if vendors are required to lock-down the ability to update firmware, they are unlikely to provide researchers or other parties with timely and effective access to mechanisms by which they might update firmware in pursuit of their research and innovation activities. This is because it represents a cost to them in time and materials, as well as supporting the use of older devices over time, because new and improved firmware is available.

4. The presence of uncorrected and uncorrectable security issues will place American interests at unnecessary risk, by preventing them from accessing security fixes provided by 3rd parties that would otherwise improve the security of their equipment. Given the continuing upward trend of cyber-espionage and other digitally-mediated crimes, both domestic and precipitated by overseas parties, this seems to create an unnecessary risk, which would otherwise require the purchase of further equipment, which in turn will have its own security issues (possible even the same vulnerabilities), rather than allowing consumers and businesses using such equipment to freely (both in terms of cost as well as liberty) access 3rd-party updates that would help to protect their interests.

5. Locking down firmware will prevent many forms of American innovation using wireless equipment, in particular by small and medium enterprises, as well as individuals and start-ups, by greatly increasing the cost of developing novel wireless technologies, services and other goods

based on low-cost wireless equipment. However, overseas innovators, not subject to the rules in their own jurisdictions, will not be hindered in this way, and will thus enjoy a completely avoidable competitive advantage over their American counterparts.

6. During emergencies and disasters both amateur radio operators and technology interest groups continue to play a significant role in providing communications in and around these theaters. In many cases, this involves the use of low-cost wireless routers and other equipment, which are re-flashed to include mesh and ad-hoc routing protocols, or in the case of amateur radio operators, to adjust the operating frequencies and/or transmit power to match the licenses under which those parties operate. The introduction of the proposed rule would effectively prevent such parties from providing this public good. Even if vendors were cooperative in providing access to their firmware update processes, it seems implausible to expect that they would be able to respond in a sufficiently timely manner. This includes activities such as the Serval Project which I lead, and is funded by the US Government via USAID.

7. Where the firmware that ships with a wireless device causes it to operate in an illegal manner, preventing the user from being able to apply 3rd-party firmware updates that correct this misbehaviour leaves them in an untenable position, with ceasing to use the equipment as their only legal option until the vendor provides an update, which as noted above, is unlikely to be forthcoming.

8. Related to the above point, if the vendor has certified that their firmware is compliant with FCC regulations, and in fact is not compliant, and they prevent consumers from applying 3rd-party updates, then the likelihood of harmful interference is increased. That is, there are mechanisms by which the rule will have the opposite effect to that intended. This also potentially raises issues of increased liability for the vendors, because they will be solely responsible for the interference caused, and may become the subject of law suits by consumers who are penalised for creating interference, or are forced to cease using their device because of uncorrectable defects in the firmware. The mere existence of this risk will increase costs for vendors, and ultimately for consumers.

9. A number of businesses buy wireless routers, reflash them with a custom firmware image, and then sell or rent them to consumers, for example, to provide internet access in rural areas. This is a valuable public good that would be completely, and presumably unintentionally, prevented by the current proposed rule.

10. In terms of the interference caused by wireless devices to date, my understanding is that an analysis of the complaint data will show that illegal operation by commercial wireless operators is a leading cause, along with importation of non-FCC approved equipment, and that there is a complete or near-complete absence of complaints that can be traced to consumers, researchers and other innovators having re-flashed their devices. Thus the rule would prevent a number of public goods, while not actually addressing the overwhelming sources of interference.

11. The importation of non-FCC approved equipment is likely to increase if this rule is adopted, because such equipment will be cheaper, due to the absence of the impact of this rule on products designed for other markets, thus contributing to that source of interference.

12. I understand the protection of the integrity of weather radars at a number of airports to be a driver for the adoption of this rule. As I have described in several of the points above, it seems unwise to assume that this rule will actually make a positive impact on that situation, given that 3rd-party firmware is rarely if ever the origin of interference. Instead, the adoption of such a rule which stimulates importation of products intended for other markets due to lower cost is a much greater

risk.

13. I understand that the zones around the several dozen airports where this is a concern are of the order of one mile in width, and thus constitutes somewhere around 1,000 square miles of the continental USA. It thus seems, given the potential negative (and in some cases self-defeating) effects of the proposed rule are also poorly targetted and disproportionate.

There are almost certainly lower-cost approaches that will instead have a positive impact on preventing this potential interference problem.

First, given the small number of airports that apparently operate weather radar in the band in question, it would seem that there are weather radar solutions that operate in other bands. Given the public safety nature of such services, it seems that it may make more sense to arrange for those relatively few airports to upgrade their weather radars over the medium term to completely eliminate the risk. This is consistent with the heirarchy of control under various health and safety regimes around the world where elimination of risk (in this case through physical separation of frequency allocations) is the highest priority, and administrative control (such as making it difficult to change the firmware) is one of the lowest priority controls – precisely because history has shown that administrative controls are a poor and relatively ineffective mechanism for maintaining safety.

Second, it would be possible to operate a radio beacon at each affected installation that provides a sentinel signal which is receivable by all devices within the necessary range, and instead require that wireless devices operating in the band in question cease transmission if they are able to receive sentinel signal. This could be implemented in hardware, thus taking enforcement of the separation out of the firmware and placing it firmly where it cannot be subverted or interfered with by any party whatever. Concerns about the inability of a sentinel signal to be received by devices deep inside buildings are greatly mitigated by two factors: (1) the reality that if a strong sentinel signal from the airport cannot be received at that location, then the ability of that wireless device transmitting at relatively low power to interfere with the weather radar is also greatly diminished; and (2) if there are black-spots for the sentinel signal, then additional sentinel transmitters could be placed to eliminate those black-spots. The sentinel could be a narrow-band low-bit-rate signal on frequency that has superior propagation characteristics to the band used for the weather radar to minimise the spectral resources required, and to further minimise the concerns already addressed above. The design of the signal should be made to minimise the cost of the receiver-side, so as to minimise the collateral cost to society through increased cost of wireless equipment.

It is true that such a strategy would introduce a cost for those few airports operating weather radar in the band in question. However, I would argue that the cost to the nation is lower to take measures to completely eliminate the problem at its origin through reallocation of the operating frequency of those radars, or to introduce a sentinel signal system, than to create a situation where public safety is risked in any way through the dependence on poorly maintained vendor firmware.

14. The costs to businesses through the requirement to recertify all existing products before June 2016 would seem likely result in a higher cost to society than the cost of addressing the operating frequency of the weather radars. Thus it is possible that the cost-benefit of the proposed rule is deficit even when considered over a 12-month period.

15. Many wireless products use components licensed under the GNU General Public License version 3 (GPLv3). Products would have to cease using those components due to the anti-Tivoization provisions of the GPLv3. This would represent a further significant cost to vendors.

16. The very real costs identified in the above two points, together with those previously described,

add further weight to the argument that the competitiveness of US vendors will be harmed, and that the result will be increased black and grey import of non-FCC-certified product, further undermining the intended effect of the rule.

17. Users sensitive to potential surveillance by foreign agencies will be unable to replace their firmware on their devices to ensure that they are running firmware that can be audited and known to be clean.

Indeed, it would seem that a simple requirement to have users enter their latitude and longitude into the router when first configuring it would be a much cheaper and at least as effective means of reducing potential interference with the weather radars than what is currently proposed. Alternatively, or in combinations with this, one could require such wireless devices to use any internet connection to periodically determine its location using one of the well-known IP-location services, and using the result to avoid interfering with the weather radar. As an alternative administrative control it would be cheap and less burdensome for vendors to implement, and could provide an explanation to users as to why this is important, and would not create the various forms of competitive disadvantage for American businesses and innovation.

While it would not offer a cast-iron guarantee that interference would not happen, these alternative approaches would not be creating a false impression of such a guarantee, in contrast to the current proposed rule that would have negligible impact on the major sources of interference, and instead create a number of negative and unintended effects on innovation, business competitiveness, humanitarian responses and endeavours as well as national security.

Thank you for considering the content of my submission, and I trust that the FCC will be able to propose an improved proposed rule that prevents the various forms of collateral damage described above, and that also provides a much stronger result for the protection of the integrity of airport weather radar.

Dr. Paul Gardner-Stephen,
President, Serval Project Inc.,
Senior Lecturer, Flinders University.
Shuttleworth Telecommunications Fellow.
paul.gardner-stephen@flinders.edu.au
+61 427 679 796

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Nicolas
Last Name: Dodu
Mailing Address: 17 rue Marcel Pagnol
City: Avrill
Country: France
State or Province: Maine-et-Loire
ZIP/Postal Code: 49240
Email Address: chaosfrogg@live.fr
Organization Name:
Comment: I'm not an American, just a web user and a "geek" like you. I think this is a very bad idea to prevent changing the firmware of wireless devices.
Indeed, this will allow any Governement install backdoor and spy on people. As well as prevent the development (eg by correcting bugs and other flaws) of the material that we belong WE bought with OUR money.
I know my voice is a dust in your Governement, but this project will touch the world indirectly. Thanks for reading me.

I'm not an American, just a web user and a "geek" like you. I think this is a very bad idea to prevent changing the firmware of wireless devices.
Indeed, this will allow any Governement install backdoor and spy on people. As well as prevent the development (eg by correcting bugs and other flaws) of the material that we belong WE bought with OUR money.
I know my voice is a dust in your Governement, but this project will touch the world indirectly. Thanks for reading me.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Richard
Last Name: Koplow
Mailing Address: 207 Reading Terrace
City: Rockville
Country: United States
State or Province: MD
ZIP/Postal Code: 20850
Email Address: captainfepa@netscape.net
Organization Name: Self
Comment:

As an IT security professional, I am very concerned that this rule might prompt manufacturers to restrict all modification to devices such as wifi systems as the easier approach, rather than simply to transmitter control.

Also, this would seem to make impermissible widely used device control software (such as Open-WRT and DD-WRT) which often is used to replace buggy, rarely updated, and non-functional OEM software.

OEMs do not seem to care about actual usability, especially in advanced applications, once their equipment is sold. The availability of open sourced software is a significant benefit to both general usability and to development of enhanced security controls.

While the proposal might not strictly disallow security improvements, the broad apparent sweep of coverage will certainly cause OEMS to lock their systems against innocous non-OEM upgrades and development.

//

I fully support the comments of the Free Software Foundation, the EFF, Open WRT, and even manufacturer Qualcomm who understand the far-reaching and very negative effects of this proposal.

As an IT security professional, I am very concerned that this rule might prompt manufacturers to restrict all modification to devices such as wifi systems as the easier approach, rather than simply to transmitter control.

Also, this would seem to make impermissible widely used device control software (such as Open-WRT and DD-WRT) which often is used to replace buggy, rarely updated, and non-functional OEM software.

OEMs do not seem to care about actual usability, especially in advanced applications, once their equipment is sold. The availability of open sourced software is a significant benefit to both general usability and to development of enhanced security controls.

While the proposal might not strictly disallow security improvements, the broad apparent sweep of coverage will certainly cause OEMS to lock their systems against innocous non-OEM upgrades and development.

//

I fully support the comments of the Free Software Foundation, the EFF, Open WRT, and even manufacturer Qualcomm who understand the far-reaching and very negative effects of this proposal.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Kevin
Last Name: DAN
Mailing Address: 20 Rue d'Ille et Vilaine
City: RENNES
Country: France
State or Province: French Brittany
ZIP/Postal Code: 35200
Email Address:
Organization Name:
Comment: don't be silly, THIS IS NOT a good idea... this is bad, very bad...

How could we update the software if there is security flaws ?? don't be silly THERE WILL HAVE SECURITY FLAWS on our devices !

don't be silly, THIS IS NOT a good idea... this is bad, very bad...

How could we update the software if there is security flaws ?? don't be silly THERE WILL HAVE SECURITY FLAWS on our devices !

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Branden
Last Name: Ray
Mailing Address: 8512 Lyn Ave
City: Savannah
Country: United States
State or Province: GA
ZIP/Postal Code: 31406
Email Address: theoriginaltrueblue@gmail.com
Organization Name:
Comment: This act is a distinct violation of our personal freedoms. When a product is purchased, it is expected that we will have the freedom to use it in the way we wish. Losing this ability would be incredibly detrimental to the American people in many ways, such as losing the ability to patch holes in security left by manufacturers, and being able to fix issues with wi-fi drivers. In addition, this act would hinder the advancement of wi-fi technology. Developers need the ability to modify their hardware and software to test new technology. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. There is no evidence leading someone to believe open-source software causes more wireless interference than closed-source. This act is completely unamerican, and will only serve to hold back technology and limit consumers.

This act is a distinct violation of our personal freedoms. When a product is purchased, it is expected that we will have the freedom to use it in the way we wish. Losing this ability would be incredibly detrimental to the American people in many ways, such as losing the ability to patch holes in security left by manufacturers, and being able to fix issues with wi-fi drivers. In addition, this act would hinder the advancement of wi-fi technology. Developers need the ability to modify their hardware and software to test new technology. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. There is no evidence leading someone to believe open-source software causes more wireless interference than closed-source. This act is completely unamerican, and will only serve to hold back technology and limit consumers.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Nazia
Last Name: Nishat
Mailing Address: 2/8/B-1,Tolarbag,Mirpur-1,Dhaka
City: Dhaka
Country: Bangladesh
State or Province: Dhaka
ZIP/Postal Code: 1216
Email Address: nazia.swe@daffodilvarsity.edu.bd
Organization Name: Daffodil Int University
Comment: I object this because security and privacy is important to me.

I object this because security and privacy is important to me.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Thomas
Last Name: Kent
Mailing Address: 1537 Moore Pl
City: University City
Country: United States
State or Province: MO
ZIP/Postal Code: 63130
Email Address: teeks99@yahoo.com
Organization Name: null
Comment: This rule would impose an overbearing penalty on the community of users who create software for home routers, wifi access points, and other equipment that utilizes open spectrum. I agree that there is a danger in allowing users to modify equipment via software to broadcast on spectrum that is outside what is legally allowed, however *there is no solution to this problem that will not adversely affect the open source community*. Therefore, I would ask the commission to reject this rule and not change the way wireless device software is regulated.

There is no fundamental difference between a user modifying software in a device, and the user opening it up and soldering transistors onto the transmitter to change its frequency.

This rule would impose an overbearing penalty on the community of users who create software for home routers, wifi access points, and other equipment that utilizes open spectrum. I agree that there is a danger in allowing users to modify equipment via software to broadcast on spectrum that is outside what is legally allowed, however *there is no solution to this problem that will not adversely affect the open source community*. Therefore, I would ask the commission to reject this rule and not change the way wireless device software is regulated.

There is no fundamental difference between a user modifying software in a device, and the user opening it up and soldering transistors onto the transmitter to change its frequency.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Etienne
Last Name: CHAMPETIER
Mailing Address: _
City: Lyon
Country: France
State or Province: _
ZIP/Postal Code: 69004
Email Address: champetier.etienne@gmail.com
Organization Name:
Comment: I'm Etienne, a french citizen.
By preventing firmware modification to wireless product sold in the US, you will prevent it worlwide, because manufacturer do not produce US and non US version.
I'm an heavy user of OpenWRT, and I care about the ability to change the firmware running on my device because:
-it's more stable (cheap devices often come with unreliable firmware)
-i have way more features (multiple ssid, ospf routing, ...)
-i can update my devices / fix security issues, all products have an eol by the manufacturer, but they still work, there is no need to produce electronic waste or let my devices be part of a botnet

I don't know any study showing that open-source firmware are causing more (or less) wireless interference than closed-source firmware, so this regulation will just prevent researchers to do their job, and increase cyberthreats (by preventing updates), without providing any advantages.

Regards
Etienne

I'm Etienne, a french citizen.
By preventing firmware modification to wireless product sold in the US, you will prevent it worlwide, because manufacturer do not produce US and non US version.
I'm an heavy user of OpenWRT, and I care about the ability to change the firmware running on my device because:
-it's more stable (cheap devices often come with unreliable firmware)
-i have way more features (multiple ssid, ospf routing, ...)
-i can update my devices / fix security issues, all products have an eol by the manufacturer, but they still work, there is no need to produce electronic waste or let my devices be part of a botnet

I don't know any study showing that open-source firmware are causing more (or less) wireless interference than closed-source firmware, so this regulation will just prevent researchers to do their job, and increase cyberthreats (by preventing updates), without providing any advantages.

Regards
Etienne

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jeff
Last Name: Freedman
Mailing Address: 213 Elm Avenue
City: Yardley
Country: United States
State or Province: PA
ZIP/Postal Code: 19067
Email Address: jeff@ifreedman.net
Organization Name:
Comment: I am a Chief Technology Officer, an IT professional with a B.S. in Computer Science and a M.S. in Information Technology Leadership with almost 30 years of professional IT experience.

Please not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points you should consider:

- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- Consumers should have the right to modify the software to their choosing so long as those modifications do not violate existing laws such as FCC channel regulation.
- Doing so puts consumers at the mercy of manufacturers with the sole charter of deciding software functionality, features and availability on devices. This severely limits consumer choice and freedom.

Thank you.

I am a Chief Technology Officer, an IT professional with a B.S. in Computer Science and a M.S. in Information Technology Leadership with almost 30 years of professional IT experience.

Please not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Additional points you should consider:

- Wireless networking research depends on the ability of researchers to investigate and modify their devices.
- Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
- Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
- Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
- Consumers should have the right to modify the software to their choosing so long as those modifications do not violate existing laws such as FCC channel regulation.
- Doing so puts consumers at the mercy of manufacturers with the sole charter of deciding software functionality, features and availability on devices. This severely limits consumer choice and freedom.

Thank you.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Greg
Last Name: Stamper
Mailing Address: 103 Val Del Ct.
City: Garner
Country: United States
State or Province: NC
ZIP/Postal Code: 27529
Email Address:
Organization Name:
Comment: These rules are stupid because they explicitly forbid open source firmware, or end user modification of firmware. Anyone with a modicum of experience in IT or wireless networks who wasn't a product of rampant cronyism or one of the myriad political lobbies with ulterior motives would have seen this coming and pointed it out.

These rules are stupid because they explicitly forbid open source firmware, or end user modification of firmware. Anyone with a modicum of experience in IT or wireless networks who wasn't a product of rampant cronyism or one of the myriad political lobbies with ulterior motives would have seen this coming and pointed it out.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: FRANCOIS
Last Name: DIRO
Mailing Address: skyleeder@live.fr
City: PARIS
Country: France
State or Province: BRETAGNE
ZIP/Postal Code: 75018
Email Address:
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Not fixing security holes either feeds cyberthreats or increases electronic waste.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

There is no evidence that open-source firmware has caused any more wireless interference than closed-source firmware.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: legros
Last Name: pierre
Mailing Address: 57 rue du pere corentin
City: paris
Country: France
State or Province: ile de france
ZIP/Postal Code: 75014
Email Address: koalassoupi@gmail.com
Organization Name:
Comment: il faut rflchir avant de faire des connerie ! niveau scurirt au bout de peux de temps cela va etre drole. et puis je pense que dans l'avenir avec se genre lois vous aller perdre le monopole de d'informatique.

il faut rflchir avant de faire des connerie ! niveau scurirt au bout de peux de temps cela va etre drole. et puis je pense que dans l'avenir avec se genre lois vous aller perdre le monopole de d'informatique.